Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program

National Institute of Standards and Technology
Communications Security Establishment

Initial Release: March 28, 2003

Last Update: September 22, 2004

Table of Contents

Overview

This Implementation Guidance document is issued and maintained by the U.S. Government's National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) of the Government of Canada, which serve as the validation authorities of the Cryptographic Module Validation Program (CMVP) for their respective governments. The CMVP is a program under which National Voluntary Laboratory Accreditation Program (NVLAP) accredited Cryptographic Module Testing (CMT) laboratories test cryptographic modules for conformance to Federal Information Processing Standard Publication (FIPS) 140-2, *Security Requirements for Cryptographic Modules*. In addition, this program covers the testing of FIPS Approved cryptographic algorithms, including the Advanced Encryption Standard, Data Encryption Algorithm, Digital Signature Algorithm, Secure Hash Algorithm, and Skipjack Algorithm.

This document is intended to provide clarifications of the CMVP, and in particular, clarifications and guidance pertaining to the *Derived Test Requirements for FIPS PUB 140-2* (DTR), which is used by CMT laboratories to test for a cryptographic module's conformance to FIPS 140-2. Guidance presented in this document is based on responses issued by NIST and CSE to questions posed by the CMT labs, vendors, and other interested parties. *However, information in this document is subject to change by NIST and CSE.*

Each section of this document corresponds with a requirements section of FIPS 140-2, with an additional first section containing general guidance that is not applicable to any particular requirements section. Within each section, the guidance is listed according to a subject phrase. For those subjects that may be applicable to multiple requirements areas, they are listed in the area that seems most appropriate. Under each subject there is a list, including the date of issue for that guidance, along relevant assertions, test requirements, and vendor requirements from the DTR. *(Note: For each subject, there may be additional test and vendor requirements which apply.)* Next, there is section containing a question or statement of a problem, along with a resolution and any additional comments with related information. This is the implementation guidance for the listed subject.

Below is a list of where the reader can find cryptographic modules validated to 140-1 and 140-2:

- Cryptographic Module Validation List

General Issues

G.1 Implementation guidance requests to NIST and CSE

Applicable Levels:	*ALL*
Effective Dates:	*2/25/1997-*
Last Modified:	*7/26/2004*
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

To whom should implementation guidance requests be directed? Is there a defined format for those requests?

Resolution

- *Programmatic Questions:* Questions concerning the general operation of the CMV Program can be directed to either NIST or CSE. Here are the appropriate points of contact:

  - **NIST**
    Randall J. Easter
    (301) 975-4641
    Ray Snouffer
    (301) 975-4436

  - **CSE**
    Jean Campbell
    (613) 991-8121
    Ken Lu
    (613) 991-8122

- *Test-specific Questions:* If a vendor is under contract with a CMT laboratory for FIPS 140-2 or algorithm testing, then the vendor should contact the laboratory with any questions concerning the test requirements. This allows the laboratory representatives to use their expertise in FIPS 140-2 testing to answer those questions, and it acts as a filter for NIST and CSE.

  Agencies, departments, vendors not under contract with a CMT laboratory, and CMT laboratories themselves who have specific questions about a FIPS 140-2 test requirement should contact the appropriate NIST and CSE points of contact:

  - **NIST**
    Randall J. Easter
    (301) 975-4641
    Ray Snouffer
    (301) 975-4436

  - **CSE**
    Jean Campbell
    (613) 991-8121

Ken Lu
(613) 991-8122

All CMT laboratory test-specific questions asking for specific implementation guidance shall have the following form, in order for NIST and CSE to understand the question as clearly as possible, and to provide an appropriate response:

1. Applicable statement(s) from FIPS 140-2,
2. Applicable assertion(s) from the FIPS 140-2 DTR,
3. Applicable required test procedure(s) from the FIPS 140-2 DTR,
4. A concise statement of the problem, followed by a clear and unambiguous question regarding the problem, and
5. A statement of the resolution that is being sought.

All questions should be presented in a detailed, implementation-specific format, rather than an academic or hypothetical format. This information should also include a brief non-proprietary description of the implementation and the FIPS 140-2 target security level. All of this will enable a more efficient and timely resolution of FIPS 140-2 related questions by NIST and CSE. When appropriate, NIST and CSE will derive general guidance from the problem and response, and add that guidance to this document. Note that general questions may still be submitted, but these questions should be identified as not being associated with a particular validation effort. The questions should be non-proprietary, as the response will be distributed to all CMT laboratories. Distribution may be restricted on a case-by case basis. The question(s) should be submitted to:

- **NIST**
  Randall J. Easter
  (301) 975-4641
  Ray Snouffer
  (301) 975-4436

- **CSE**
  Ghislain Lagace
  (613) 991-8497
  Jean Campbell
  (613) 991-8121

****Note that NIST and CSE will only issue official, written responses when the original request is submitted in writing (e-mail and fax are also acceptable – MS Word document preferred).*

Additional Comments

G.2 Completion of a test report: Information that must be provided to NIST and CSE

Applicable Levels:	*ALL*
Effective Dates:	*2/25/1997-01/19/2004*
Last Modified:	*1/9/2004*
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

What information should be provided to NIST and CSE upon completion of the CMT laboratory conformance testing in order for NIST and CSE to perform a validation review?

Resolution

The following information shall be provided to both NIST and CSE by the CMT laboratory:

1. **Non-proprietary Security Policy** <PDF>
   Reference FIPS 140-2 DTR and IG 14.1 for requirements. The non-proprietary security policy shall not be marked as proprietary or copyright without a statement allowing copying or distribution.

2. **CRYPTIK v5.5 (or higher) Reports**
   The validation report submission must be output from the NIST provided Cryptik tool.

   a. **Signature page / Cover Sheet** <PDF with mailed *signed* hard copy>

   b. **General Information** <PDF>

   c. **Billing for Cost Recovery** <PDF – if applicable>

   d. **Report Overview with Assessments** <PDF>

   e. **Detailed Report with Assessments** <PDF>

   f. **Certificate** <RTF>

   g. **Definitions / References** <PDF - optional>

3. **Physical Test Report** <PDF – mandatory at Levels 2, 3 and 4>
   The laboratory's physical testing report with photos, drawing, etc. as applicable.

4. **Section Summaries** <optional>
   Briefly describe how the requirements in each section are met.

The CMT laboratory has the option to additionally provide *Notes* and *Proprietary* output with the Detailed Report with Assessments, but this is not required by NIST and CSE. The Report Overview with Assessments shall not include proprietary information. The PDF files shall not be locked. All Cryptik PDF submission output, including optional section summaries and physical test report must be merged into a single PDF document.

The submission documents shall be ZIP'ed into a single file, encrypted and sent to the following NIST and CSE points of contact:

- **NIST**
  Janet Jing
  (301) 975-4293
  Randall J. Easter <on copy>
  (301) 975-4641

- **CSE**
  Ghislain Lagace
  (613) 991-8497
  Jean Campbell <on copy>

(613) 991-8121

****NOTE: The signed signature page and cost recovery fees (if applicable) must be received before a validation certificate will be issued. ****

Additional Comments

Reception of the electronic submission documents will determine position in the CMVP validation review queue, not when the hard copy signature page is received.

An Initial Review will not be performed on the submission documents.

G.3 Partial validations

Applicable Levels:	*ALL*
Effective Dates:	*2/25/1997-*
Last Modified:	
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

What is the position of NIST and CSE regarding partial validations?

Resolution

NIST and CSE will not issue a validation certificate unless a cryptographic module meets at least Level 1 security requirements for each area in Section 4 of FIPS 140-2. Note that in some cases, a requirements area might not be applicable to the cryptographic module being tested (e.g., "Mitigation of Other Attacks"). In those cases, the validation certificate will indicate "N/A" for that requirement.

Additional Comments

G.4 Design and testing of cryptographic modules

Applicable Levels:	*ALL*
Effective Dates:	*11/12/1997-*
Last Modified:	*4/28/2000*
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

What activities may CMT laboratories perform, regarding the design and testing of cryptographic modules?

Resolution

The following information is supplemental to the guidance provided by NVLAP, and further defines the separation of the design, consulting, and testing roles of the laboratories. CMV Program policy in this area is as follows:

1. A CMT Laboratory *may not* perform validation testing on a module for which the laboratory has:
    a. designed any part of the module,
    b. developed original documentation for any part of the module,
    c. built, coded or implemented any part of the module, or
    d. any ownership or vested interest in the module.
2. Provided that a CMT Laboratory has met the above requirements, the laboratory *may* perform validation testing on modules produced by a company when:
    a. the laboratory has no ownership in the company,
    b. the laboratory has a completely separate management from the company, and
    c. business between the CMT Laboratory and the company is performed under contractual agreements, as done with other clients.
3. A CMT Laboratory may perform consulting services to provide clarification of 140-2, the Derived Test Requirements, and other associated documents at any time during the life cycle of the module.

Additional Comments

Item 3 in the Resolution references "other associated documents". Included in this reference are:

- Documents developed by the CMVP staff for the Cryptographic Module testing program (e.g., Implementation Guidance, CMVP Policy, Handbook 150-17, *Cryptographic Module Testing*); and
- Implementation Guidance and Policy associated with 140-2, *Security Requirements for Cryptographic Modules*.

Also see IG G.9, regarding FSM and Security Policy consolidation and formatting.

G.5 Maintaining validation compliance of software or firmware cryptographic modules

Applicable Levels:	*ALL*
Effective Dates:	*11/12/1997-*
Last Modified:	*8/19/2004*
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

For a validated software or firmware cryptographic module, how may such a module be implemented so that compliance with the validation is maintained?

Resolution

1. The tested/validated configuration is stated on the validation certificate. The certificate serves as the benchmark for the module-compliant configuration.

2. For level 1 Operational Environment, the software cryptographic module will remain compliant with the FIPS 140-2 validation when operating on any general purpose computer (GPC) provided that:

    a. the GPC uses the specified single user operating system/mode specified on the validation certificate, or another compatible single user operating system, and
    b. the source code of the software cryptographic module does not require modification prior to recompilation to allow porting to another compatible single user operating system.

3. For level 2 Operational Environment, the software cryptographic module will remain compliant with the FIPS 140-2 validation when operating on any GPC provided that:

    a. the GPC incorporates the specified CC evaluated EAL2 (or equivalent) operating system/mode/operational settings or another compatible CC evaluated EAL2 (or equivalent) operating system with like mode and operational settings, and
    b. the source code of the software cryptographic module does not require modification prior to recompilation to allow porting to another compatible CC evaluated EAL2 operating system.

4. Software or firmware modules that require any source code modifications to be recompiled and ported to another GPC or operational environment must be reviewed by a CMT laboratory and revalidated per IG G.8 (1) [non-security relevant changes].

5. If the Operational Environment is not applicable, a firmware module and its identified unchanged tested operating system (i.e. same version or revision number) may be ported together from one GPC or platform to another GPC or platform while maintaining the module's validation. Furthermore, except for GPCs, the tested platform must also be specified on the validation certificate.

This policy only addresses the operational environment under which a software or firmware module executes and does not affect requirements of the other sections of FIPS 140-2. A module must meet all requirements of the level stated.

Additional Comments

The CMVP allows the porting of a validated software cryptographic module from the OS(s) and/or GPC(s) specified on the validation certificate to an OS(s) and/or GPC(s) which were not included as part of the validation testing. The validation status is maintained without re-testing the cryptographic module on the new OS(s) and/or GPC(s). However, the CMVP makes no statement as to the correct operation of the module when ported to an OS(s) and/or GPC(s) not listed on the validation certificate.

Please see IG 1.3 *Firmware Designation* regarding difference in terminology between a *software* and a *firmware* module.

*Note that this guidance is particularly relevant to **USERS** who are implementing a software or firmware module.*

G.6 Modules with both a FIPS mode and a non-FIPS mode

(i.e., modules containing both FIPS-approved and non-FIPS approved security methods)

Applicable Levels:	*ALL*
Effective Dates:	*3/11/1998-*
Last Modified:	*4/2/1998*
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

How can a module be defined, when it includes both FIPS-approved and non-FIPS approved security methods?

Resolution

(4/2/98) A module that contains both FIPS-approved and non-FIPS approved security methods shall have at least one "FIPS mode of operation" - which *only* allows for the operation of FIPS-approved security methods. This means that when a module is in the "FIPS mode", a non-FIPS approved method **SHALL NOT** be used in lieu of a FIPS-approved method (For example, if a module contains both MD5 and SHA-1, then when hashing is required in the FIPS mode, SHA-1 must be used.). The operator must be made aware of which services are FIPS 140-2 compliant.

The FIPS 140-2 validation certificate will identify the cryptographic module's "FIPS mode" of operation.

The selection of "FIPS mode" does not have to be restricted to any particular operator of the module. However, each operator of the module must be able to determine whether or not the "FIPS mode" is selected.

There is no requirement that the selection of a "FIPS mode" be permanent.

Additional Comments

G.7 Relationships Among Vendors, Laboratories, and NIST/CSE

Applicable Levels:	*ALL*
Effective Dates:	*4/14/1998-*
Last Modified:	
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

What is the Cryptographic Module Validation Program policy regarding the relationships among vendors, testing laboratories, and NIST/CSE?

Resolution

The CMT laboratories are accredited by NVLAP to perform cryptographic module validation testing to determine compliance with FIPS 140-2. NIST/CSE rely on the CMT laboratories to use their extensive validation testing experience and expertise to make sound, correct, and independent decisions based on 140-2,

the Derived Test Requirements, and Implementation Guidance. Once a vendor is under contract with a laboratory, NIST/CSE will only provide official guidance and clarification for the vendor's module through the point of contact at the laboratory.

In a situation where the vendor and laboratory are at an irresolvable impasse over a testing issue, the vendor may ask for clarification/resolution directly from NIST/CSE. The vendor should use the format required by Implementation Guidance G.1 and the point of contact at the laboratory ***must*** be carbon copied. All correspondence from NIST/CSE to the vendor on the issue will be issued through the laboratory point of contact.

Additional Comments

G.8 Revalidation Requirements

Applicable Levels:	*ALL*
Effective Dates:	*8/17/2001-*
Last Modified:	*4/4/2003*
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

What is the Cryptographic Module Validation Program (CMVP) policy regarding revalidation requirements and validation of a new cryptographic module that is significantly based on a previously validated module?

Resolution

An updated version of a previously validated cryptographic module can be considered for a revalidation rather than a full validation depending on the extent of the modifications from the previously validated version of the module. (Note: the updated version may be, for example, a new version of an existing crypto module or a new model based on an existing model.)

There are four possible scenarios:

1. Modifications are made to hardware, software or firmware components that do not affect any FIPS 140-2 security relevant items. The CMT laboratory is responsible for identifying the necessary documentation to confirm that FIPS 140-2 security relevant items have not been affected by the modification. The vendor is then responsible to provide the applicable documentation to the CMT laboratory. Documentation may include a previous validation report, design documentation, source code, etc. The CMT laboratory will review the modifications and any associated documentation provided by the vendor and issue an explanatory letter to NIST/CSE with applicable TEs listed and associated laboratory assessment. The assessment shall include the analysis performed by the laboratory to confirm that no security relevant TEs were affected. The updated version or release information will be posted on the FIPS 140-2 Cryptographic Module Validation List entry associated with the original cryptographic module. No new certificate will be issued.
2. Modifications are made to hardware, software or firmware components that affect some of the FIPS 140-2 security relevant items. An updated cryptographic module can be considered in this scenario if it is similar to the original module with only minor changes in the security policy and FSM, and less than 30% of the assertions in the FIPS 140-1 conformance test report are affected. The CMT laboratory is responsible for identifying the documentation that is needed to determine whether a revalidation is sufficient and the vendor is responsible for submitting the requested documentation to

the CMT laboratory. Documentation may include a previous validation report and applicable NIST/CSE rulings, design documentation, source code, etc.

The CMT laboratory shall identify the assertions affected by the modification and shall perform the tests associated with those assertions. This will require the CMT lab to:

1. Review the COMPLETE list of assertion for the module embodiment and security level,
2. Identify, from the previous validation report, the assertions that have been affected by the modification,
3. Identify additional assertions that were NOT previously tested but should now be tested due to the modification, and
4. Review assertions where specific Implementation Guidance (IG) was provided to confirm that the IG is still applicable.

For example, a revision to a firmware component that added security functionality may require a change to assertions in Section 1.

In addition to the tests performed against the affected assertions, the CMT laboratory shall also perform the regression test suite of operational tests included in **Mapping FIPS 140-2 to FIPS 140-1**. Included in the table are the ASs, TEs, VEs (AS2 for FIPS 140-2 and AS1 for FIPS 140-1, etc.), security level(s), single chip (S), multi chip embedded (ME), multi chip standalone (MS), operational test (op - x is used for the operational tests, r is used for regression test), applicable to FIPS 140-2 (M - match), and comment (describes the applicability of FIPS 140-1 results to 140-2, and may include info on the 140-2 requirement).

The CMT laboratory shall document the test results in the associated assessments and all affected TEs shall be annotated as "re-tested." The CMT laboratory can submit a delta conformance test report highlighting those assertions that have been modified and retested. Upon a satisfactory review by NIST/CSE, a new certificate will be issued.

3. Modifications are made only to the physical enclosure of the cryptographic module that provides its protection and involves no operational changes to the module. The CMT laboratory is responsible for ensuring that the change only affects the physical enclosure (integrity) and has no operational impact on the module. The CMT laboratory must also fully test the physical security features of the new enclosure to ensure its compliance to the relevant requirements of the standard. The CMT laboratory must then submit a letter to NIST and CSE that:

    1. Describes the change (pictures may be required),
    2. State that it is a security relevant change.
    3. Provide sufficient information supporting that the physical only change has no operational impact,
    4. Describes the tests performed by the laboratory that confirms that the modified enclosure still provides the same physical protection attributes,

    Each request will be handled on a case-by-case basis. The CMVP will accept such letters against cryptographic modules already validated to FIPS 140-1 and FIPS 140-2. Certificates will not be reissued.

    An example of such a change could be a Level 2 tokens plastic encapsulation that has been reformulated or colored. Therefore the molding or cryptographic boundary has been modified. This

change is security relevant as the encapsulation provides the opacity and tamper evidence requirements. But this can be handled as a letter only change with evidence that the new composition has the same physical security relevant attributes as the prior composition.

4. If modifications are made to hardware, software, or firmware components that do not meet the above criteria, then the cryptographic module will be considered a new module and must undergo a full validation testing by an accredited CMT laboratory.

If the overall Security Level of the crypto module changes or if the physical embodiment changes, e.g., from multi-chip standalone to multi-chip embedded, then the cryptographic module will be considered a new module and must undergo full validation testing by an accredited CMT laboratory.

Additional Comments

A cryptographic module that is revalidated must meet ALL current standards and IGs. The CMT laboratory is responsible for requesting from the vendor all the documentation necessary to determine whether the cryptographic module meets the current standards and IGs. This is particularly important for features/services of the cryptographic module that required a specific ruling from NIST/CSE. For example, a cryptographic module may have been validated with an implementation of Triple DES that has not been tested. If the same cryptographic module is later submitted for revalidation, this Triple DES implementation must be tested and validated against FIPS 46-3, and the cryptographic module must meet the applicable FIPS 140-2 requirements, e.g., self-tests.

G.9 FSM, Security Policy, User Guidance and Security Officer Guidance Documentation

Applicable Levels:	ALL
Effective Dates:	5/29/2002
Last Modified:	
Relevant Assertions:	
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

May a CMT lab create original documentation specified in FIPS 140-2? The specific documents in question are the FSM, Security Policy, User Guidance and Security Officer Guidance.

Resolution

FSM and Security Policy:

A CMT lab may take existing vendor documentation for an existing cryptographic module (post-design and post-development) and consolidate or reformat the existing information (from multiple sources) into a set format. If this occurs, NIST and CSE shall be notified of this when the validation report is submitted. Additional details for the individual documents are provided below.

FSM: The vendor-provided documentation must readily provide a finite set of states, a finite set of inputs, a finite set of outputs, a mapping from the sets of inputs and states into the set of states (i.e., state transitions), and a mapping from the sets of inputs and states onto the set of outputs (i.e., an output function).

Security Policy: The vendor-provided documentation must readily provide a precise specification of the security rules under which a cryptographic module must operate, including the security rules derived from the requirements of FIPS 140-2 and the additional security rules imposed by the vendor.

In addition, a lab must be able to show a mapping from the consolidated or reformatted FSM and/or Security Policy back the original vendor source documentation. The mapping(s) must be maintained by the lab as part of the validation records.

Consolidating and reforming are defined as follows:

- The original source documents were prepared by the vendor (or a subcontractor to the vendor) and submitted to the laboratory with the cryptographic module.
- The laboratory extracts applicable technical statements from the original source documentation to be used in the FSM and/or Security Policy. The technical statements may **only** be reformatted to improve readability of the FSM and/or Security Policy. The content of the technical statements must not be altered.
- The laboratory may develop transitional statements in the FSM and/or Security Policy to improve readability. These transitional statements shall be specified as developed by the laboratory in the mapping.

User Guidance and Security Officer Guidance:

A CMT lab may create User Guidance, Security Officer Guidance and other non-design related documentation for an existing cryptographic module (post-design and post-development). If this occurs, NIST and CSE shall be notified of this when the validation report is submitted.

Additional Comments

G.10 Physical Security Testing for Re-validation from FIPS 140-1 to FIPS 140-2

Applicable Levels:	*ALL*
Effective Dates:	*3/29/2004*
Last Modified:	
Relevant Assertions:	
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Background

FIPS 140-2 IG G.2 specifies that all report submissions must include a separate physical security test report section for Levels 2, 3 or 4.

Question/Problem

Questions have been asked regarding re-validation test reports where a previous separate physical security test report may not have existed or evidence such as images, etc. had not been provided with the original validation test report. What should the CMT laboratory provide if the physical security requirements have not changed?

Resolution

If a previous *separate* physical security test report did not exist for the module undergoing re-validation testing and the physical security features of the module have not changed, the CMT Laboratory must compile the physical security test evidence that has been maintained from their records from the original tested module and create and submit a new *separate* physical security test report. If the records no longer exist because they were generated outside the period of the CMT Laboratories record retention period specified in the quality manual, then re-testing shall be required to provide such evidence. It is not required that a CMT laboratory perform re-testing simply to create new photographic images that may not have been saved or generated during the original testing

Additional Comments

If the CMT Laboratory was not the original testing laboratory and therefore does not have access to the previous test records, then the module shall be re-tested to be able to provide such evidence. Without the prior records, the new CMT Laboratory cannot make a determination that the physical security has or has not changed.

Section 1 - Cryptographic Module Specification

1.1 Cryptographic Module Name

Applicable Levels:	*ALL*
Effective Dates:	*2/27/2004*
Last Modified:	
Relevant Assertions:	*AS.01.05, AS.01.08 and AS.01.09*
Relevant Test Requirements:	*TE.01.08.03, 04 and 05 and TE.01.09.01 and 02*
Relevant Vendor Requirements:	*VE.01.08.03 and VE.01.09.01*

Question/Problem

How shall the name of a cryptographic module relate to the defined cryptographic boundary?

Resolution

The provided name of the cryptographic module (which will be on the validation certificate) shall be consistent with the defined cryptographic boundary as defined in the test report.

It is not acceptable to provide a module name that represents a module that has more components than the modules defined boundary. If it is desired to have a name that does represent a larger entity, then the cryptographic boundary must be consistent. All components residing within the cryptographic boundary must either be included (**AS.01.08**) or excluded (**AS.01.09**) in the test report.

Additional Comments

Example: The provided name of a cryptographic module is the *Crypto Card*. However, the defined cryptographic boundary in the test report is a small black encapsulated component placed in one corner of the card. The named card also has additional components that were not referenced (e.g. batteries, connectors). If the defined boundary in the test report specifies *ONLY* the black encapsulated component, it is clearly NOT the *Crypto Card*. A unique different name shall be provided to be consistent with the defined boundary. To represent the entire card, the boundary must be redefined and must include all the components and address them properly (include/exclude).

1.2 FIPS Approved Mode of Operation

Applicable Levels:	*ALL*
Effective Dates:	*3/15/2004*
Last Modified:	
Relevant Assertions:	*AS.01.02, AS.01.03 and AS.01.04*
Relevant Test Requirements:	*TE.01.03.01 and 02 and TE.01.04.01 and 02*
Relevant Vendor Requirements:	*VE.01.03.01 and 02 and VE.01.04.01 and 02*

Definition

Approved mode of operation: a mode of the cryptographic module that employs only Approved security functions (not to be confused with a specific mode of an Approved security function, e.g., DES CBC mode).

Question/Problem

Are there any operational requirements when switching between modes of operation, either from an Approved mode of operation to a non-Approved mode of operation, or vice versa?

Resolution

In addition to the requirements specified in AS01.02, AS.01.03 and AS.01.04, a module shall not share CSPs between modes of operation, (i.e., Approved mode of operation and a non-Approved mode of operation).

Additional Comments

This separation mitigates the risk of untrusted handling of CSPs generated in an Approved mode of operation. Examples:

- a module may not generate keys in a non-Approved mode of operation and then switch to an Approved mode of operation and use the generated keys for Approved services. The keys may have been generated using non-Approved methods and their integrity and protection cannot be assured.
- a module shall not electronically import keys in plain text in a non-Approved mode of operation and then switch to an Approved mode of operation and use those keys for Approved services.
- a module may not generate keys in an Approved mode of operation and then switch to a non-Approved mode of operation and use the generated keys for non-Approved services. The integrity and the protection of the Approved keys cannot be assured in the non-Approved mode of operation.

1.3 Firmware Designation

Applicable Levels:	*ALL*
Effective Dates:	*4/28/2004*
Last Modified:	
Relevant Assertions:	*AS.01.01*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Background

Cryptographic module: the set of hardware, software, and/or firmware that implements Approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.

Firmware: the programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) within the cryptographic boundary and cannot be dynamically written or modified during execution.

The *operational environment* of a cryptographic module refers to the management of the software, firmware, and/or hardware components required for the module to operate. The operational environment can be non-modifiable (e.g., firmware contained in ROM, or software contained in a computer with I/O devices disabled), or modifiable (e.g., firmware contained in RAM or software executed by a general purpose computer).

A *limited operational environment* refers to a static non-modifiable virtual operational environment (e.g., JAVA virtual machine on a non-programmable PC card) with no underlying general purpose operating system upon which the operational environment uniquely resides.

If the operational environment is a limited operational environment, the operating system requirements in Section 4.6.1 do not apply.

Question/Problem

How shall a *software* cryptographic module running on a limited operational environment be designated as?

Resolution

If the Operational Environment is a limited operational environment, and is indicated as NA on the certificate, then the cryptographic module shall be designated as a ***firmware*** module.

Additional Notes

- The reference tested OS must be indicated on the validation certificate for all software and firmware cryptographic modules. It will be referenced on the CMVP validation list web page as follows:
  - If the Operational Environment is applicable: -*Operational Environment: Tested as meeting Level x with ...*
  - If the Operational Environment is NA: -*Tested: ...*
- For a Level 2 module, the reference hardware platform used during operational testing must also be listed.
- For JAVA applets, the tested JAVA environment (JRE, JVM) and operating system need to be specified for all Security Levels.

Per FIPS 140-2 IG G.5, porting of software modules is only applicable to modules operating on a General Purpose Computer (GPC) and when the Operational Environment is applicable. The module's validation will be maintained if no changes are made to underlying source code.

If the operational environment is not applicable, a firmware module and its identified tested OS together may be ported from one platform to another platform while maintaining the module's validation For firmware module's that are JAVA applets, the firmware module, its identified tested OS, and the tested JAVA environment (JRE, JVM) must be moved together when porting from one platform to another platform in order to maintain the module's validation.

All other cases, the validation of the cryptographic module is not maintained.

1.4 Use of Cryptographic Algorithm Validation Certificates

Applicable Levels:	*ALL*
Effective Dates:	*7/26/2004*
Last Modified:	
Relevant Assertions:	*AS01.12*
Relevant Test Requirements:	*TE01.12.01*
Relevant Vendor Requirements:	*VE0.12.01*

Background

Cryptographic algorithm implementations are tested and validated under the Cryptographic Algorithm Validation System. The cryptographic algorithm validation certificate states the name and version number of the validated implementation, and the test operational environment.

Cryptographic modules are tested and validated under the Cryptographic Module Validation Program. The cryptographic module validation certificate states the name and version number of the validated cryptographic module, and the test operational environment.

The validation certificates serve as benchmarks for the configuration and operational environment used during the validation testing.

Question/Problem

What are the configuration control and operational environment requirements for the use of cryptographic algorithm certificates (implementations) embedded within a cryptographic module when the latter is undergoing testing for compliance to FIPS 140-2?

Resolution

For a validated cryptographic algorithm implementation to be embedded within a software, firmware or hardware cryptographic module that undergoes testing for compliance to FIPS 140-2, the following requirements must be met:

1. the source code or implementation of the validated cryptographic algorithm implementation has not been modified upon integration into the cryptographic module undergoing testing; and

2. the operational environment under which the validated cryptographic algorithm implementation was tested must be identical to the operational environment that the cryptographic module is being tested under.

Additional Comments

1.5 Validation Testing of SHS Algorithms and Higher Cryptographic Algorithm Using SHS Algorithms

Applicable Levels:	*All*
Effective Dates:	*8/19/2004*
Last Modified:	
Relevant Assertions:	*AS01.12*
Relevant Test Requirements:	*TE01.12.01*
Relevant Vendor Requirements:	*VE01.12.01*

Background

The Cryptographic Algorithm Validation Program (CAVP) validates every SHS algorithm implementation: SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512. Several higher cryptographic algorithms use those SHS hashing algorithms in their operation.

Question/Problem

What are validation testing requirements for the SHS algorithms and higher cryptographic algorithms implementing SHS algorithms for their use in FIPS Approved mode of operation?

Resolution

To be used in a FIPS Approved mode of operation:

- every SHS algorithm implementation must be tested and validated on the appropriate OS.

- for DSA, RSA, ECDSA and HMAC, every implemented combination must be tested and validated on the appropriate OS.

The algorithmic validation certificate annotates all the tested implementations that may be used in a FIPS Approved mode of operation.

Any algorithm implementation incorporated within a FIPS 140-2 cryptographic module that is not tested may not be used in a FIPS Approved mode of operation. If there is an untested subset of a FIPS Approved algorithm, it would be listed as non-Approved and non-compliant on the FIPS 140-2 validation certificate.

Additional Comments

Section 2 – Cryptographic Module Ports and Interfaces

Section 3 – Roles, Services, and Authentication

3.1 Authorized Roles

Applicable Levels:	*ALL*
Effective Dates:	*5/29/2002*
Last Modified:	
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

An operator is not required to assume an authorized role to perform services where cryptographic keys and CSPs are not modified, disclosed, or substituted (e.g., show status, self-tests, or other services that do not affect the security of the module).

Resolution

Authorized roles are applicable to all callable services utilizing FIPS Approved cryptographic algorithms.

Additional Comments

Section 4 - Finite State Model

Section 5 - Physical Security

5.1 Opacity and Probing of Cryptographic Modules with Fans, Ventilation Holes or Slits at Level 2

Applicable Levels:	*2*
Effective Dates:	*2/10/2004*
Last Modified:	
Relevant Assertions:	*AS.05.49*
Relevant Test Requirements:	*TE.05.49.01*
Relevant Vendor Requirements:	*VE.05.49.01*

Background

Cryptographic modules typically require the use of heat dissipation techniques that can include the use of fans, ventilation holes or slits. The size of these openings in the modules' enclosure, or the spacing between fan blades, may allow the viewing or possible probing of internal components and structures within the cryptographic module.

Question/Problem

How do the opacity requirements of FIPS 140-2 affect the design of the heat dissipation techniques on those cryptographic modules at Security Level 2? Should the cryptographic module prevent probing through the ventilation holes or slits at Security Level 2?

Resolution

The following are the physical security requirements for multi-chip stand-alone module at Security Level 2 pertaining to opacity and probing:

- the embodiments that are entirely contained within a metal or hard plastic production-grade enclosure that may include doors or removable covers (Security Level 1 requirement); and
- the enclosure of the cryptographic module shall be opaque within the visible spectrum.

Probing Requirements

Probing is not addressed at Security Level 2. Probing through ventilation holes or slits is addressed at Security Level 3 (AS.05.21).

Opacity Requirements

The purpose of the opacity requirement is to deter direct observation of the cryptographic module's internal components and design information to prevent a determination of the composition or implementation of the module.

A module is considered “opaque” only if it cannot be determined by visual inspection within the visible spectrum using artificial light sources shining through the enclosure openings or translucent surfaces, the manufacturer and/or model numbers of internal components (such as specific IC types) and/or design and composition information (such as wire traces and interconnections).

Component outlines may be visible from the enclosure openings or translucent surfaces as long as the component’s manufacturer and/or model numbers, and/or composition and information about the module’s design cannot be determined.

All components within the boundary of the cryptographic module must meet the opacity requirements of the standard. Excluded non-security relevant components do not have to meet these requirements.

Additional Comments

Note: Visible light is defined as light within a wavelength range of 400nm to 750nm.

Section 6 – Operational Environment

6.1 Single Operator Mode and Concurrent Operators

Effective Dates:	3/10/2003
Last Modified:	4/24/2003
Relevant Assertions:	AS06.04
Relevant Test Requirements:	VE.06.04
Relevant Vendor Requirements:	TE.06.04

Background

Historically, for a FIPS 140-1 and FIPS 140-2 validated software cryptographic module on a server to meet the single user requirement of Security Level 1, the server had to be configured so that only *one* user at a time could access the server. This meant configuring the server Operating System (OS) so that only a single user at a time could execute processes (including cryptographic processes) on the server. Consequently, servers were not being used as intended.

Question/Problem

AS06.04 states: "(Level 1 Only) The operating system shall be restricted to a single operator mode of operation (i.e., concurrent operators are explicitly excluded)". What is the definition of concurrent operators in this context? Specifically, may Level 1 software modules be implemented on a server and achieve FIPS 140-2 validation? (Note: this question is also applicable to VPN, firewalls, etc.)

Resolution

Software cryptographic modules implemented in client/server architecture are intended to be used on both the client and the server. The cryptographic module will be used to provide cryptographic functions to the client and server applications. When a crypto module is implemented in a server environment, the server application is the user of the cryptographic module. The server application makes the calls to the cryptographic module. Therefore, the server application is the single user of the cryptographic module, even when the server application is serving multiple clients

Additional Comments

This information must be included in the non-proprietary security policy.

6.2 Applicability of Operational Environment Requirements to JAVA Smart Cards

Applicable Levels:	ALL
Effective Dates:	4/08/2003
Last Modified:	09/11/2003
Relevant Assertions:	AS06.01
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Background

FIPS 140-2 states (Section 4.6 Operational Environment) "A limited operational environment refers to a static non-modifiable virtual environment (e.g., a JAVA virtual machine on a non-programmable PC card) with no underlying general purpose operating system upon which the operational environment uniquely resides."

Question

Does the FIPS 140-2 statement mean that a smart card implementing a non-modifiable operating system (e.g., like the ones currently used today in most smart cards) that accept and run JAVA applets (whether validated or not) is a limited operational environment?

Resolution

The CMVP cannot issue a general statement that applies to all JAVA card modules since functionality and design can vary greatly from module to module. The determination is left to the CMT laboratories, which have the complete module documentation available to them. In general**,** however, a JAVA smart card module with the ability to load unvalidated applets post-validation is considered to have a ***modifiable*** operational environment and the Operational Environment requirements of FIPS 140-2 are applicable.

A JAVA smart card module having a modifiable operational environment which either:

a) is configured such that the loading of any applets is not possible, or

b) loads only applets that have been tested and validated to either FIPS 140-1 or FIPS 140-2,

could be considered to have a ***limited*** operational environment and have the FIPS 140-2 Operational Environment requirements section of the module test report marked as *Not Applicable*.

The validated JAVA smart card cryptographic module must use an Approved authentication technique on all loaded applets. The module shall also meet, at a minimum, the requirements of AS09.34, AS09.35, AS10.03 and AS10.04, as well as any other applicable assertions. Validation of the cryptographic module is maintained through the loading of applets that have either been tested and validated during the validation effort of the smart card itself or through an independent validation effort (i.e., the applet itself has its own validation certificate number).

The security policy of the validated smart card module must state whether:

- The module can load applets post-validation, validated or not (Note: if the module can load non-validated applets post-validation, the security policy must clearly indicate that the module's validation to FIPS 140-1 or FIPS 140-2 is no longer valid once a non-validated applet is loaded);

- Any applets are contained within the validated cryptographic module and, if so, must list their name(s) and version number(s).

Additional Comments

The name(s) and version number(s) of all applets contained within a validated cryptographic module shall be listed on the module's certificate and CMVP website entry.

6.3 Correction to Common Criteria Requirements on Operating System

Applicable Levels	ALL
Effective Dates	03/29/2004
Last Modified	
Relevant Assertions	AS.06.10, AS.06.21 and AS.06.27

Relevant Test Requirements	TE.06.10, TE.06.21 and TE.06.27
Relevant Vendor Requirements	VE.06.10, VE.06.21 and VE.06.27

Background

Depending on how assertions AS.06.10, AS.06.21 and AS.06.27 are read, they could be interpreted as the OS upon which the module is running on has to meet ALL of the listed PPs in Annex B at EAL2, EAL3 and EAL4 respectively. This is because of the plural at the end of the "Protection Profile**s**".

Question/Problem

Must the OS upon which the module is running on has to meet ALL of the listed PPs in Annex B at EAL2, EAL3 and EAL4 respectively?

Resolution

No, the requirements should be interpreted to read as follows:

- For **AS.06.10**:

  an operating system that meets the functional requirements specified in **a** Protection Profile listed in Annex B and is evaluated at the CC evaluation assurance level EAL2

- For **AS.06.21**, the first sentence:

  an operating system that meets the functional requirements specified in **a** Protection Profile listed in Annex B.

- For **AS.06.27**, the first sentence:

  an operating system that meets the functional requirements specified in **a** Protection Profile listed in Annex B.

Additional Notes

Section 7 – Cryptographic Key Management

7.1 Acceptable Key Establishment Protocols

Applicable Levels:	*ALL*
Effective Dates:	*2/10/2004*
Last Modified:	*8/19/2004*
Relevant Assertions:	*AS07.21*
Relevant Test Requirements:	*TE07.21.01*
Relevant Vendor Requirements:	*VE07.21.01 - 02*

Background

Cryptographic modules are using Secure Socket Layer (SSL), Transport Layer Security (TLS), IP Security (IPSEC) and password-based key establishment protocols to establish and maintain secure communication links between modules.

Question/Problem

Which protocols between SSL, TLS, IPSEC and password-based key establishment can be used in FIPS Approved mode of operation to establish keys to be used for data encryption and decryption?

Resolution

The following paragraphs describe the status of each protocol with reference to its usage in FIPS Approved mode of operation to establish keys to be used for data encryption and decryption:

- SSL: all versions of the SSL protocol are not to be used in FIPS mode. The manner in which the protocol uses approved and non-approved cryptographic algorithms for its operation prohibits its usage.
- TLS: the TLS protocol can be used in FIPS mode. While the protocol uses the same cryptographic algorithms as the SSL protocol, the manner in which the algorithms are used makes it acceptable to be used in FIPS mode.
- IPSEC: the IPSEC protocol can be used in FIPS mode so long as the cryptographic algorithms used by the implementation are FIPS Approved.
- Password-Based Key Establishment protocols: all password-based key establishment protocols such as PKCS#5 are not to be used in FIPS mode.

The key establishment protocol(s) used by the cryptographic module must be listed under AS.07.21.

Additional Comments

This IG does not address key establishment for use in authentication techniques.

FIPS 140-2 Annex D references Approved Key Establishment Techniques. A key establishment protocol may be comprised of several different techniques and algorithms and therefore protocols are not identified in Annex D.

Section 8 – Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

Section 9 – Self-Tests

9.1 Known Answer Test for Keyed Hashing Algorithm

Applicable Levels:	*All*
Effective Dates:	*2/10/2004*
Last Modified:	*9/22/2004*
Relevant Assertions:	*AS.09.07*
Relevant Test Requirements:	*TE.09.07.01*
Relevant Vendor Requirements:	*VE.09.07.01*

Background

Several keyed hashing algorithms are FIPS-approved (e.g. DES MAC, HMAC-SHA-1) and have different levels of complexity that determine the power-on Know-Answer-Test (KAT) requirements.

Question/Problem

What are the KAT requirements when implementing keyed hashing algorithms in FIPS mode?

Resolution

The following table summarizes the minimal KAT requirements:

KAT Requirements	Keyed Hashing algorithm	Underlying algorithm
DES MAC / Triple-DES MAC	No	Yes
HMAC-SHA-1	Yes	No
HMAC-SHA-224	Yes	No
HMAC-SHA-256	Yes	No
HMAC-SHA-384	Yes	No
HMAC-SHA-512	Yes	No

Rationale

DES MAC and the Triple-DES MAC algorithms do not include much additional complexity over the underlying algorithmic engine (e.g. DES and Triple-DES). However, keyed hashing algorithms such as HMAC-SHA-1 have additional complexity over the underlying algorithmic engine (e.g. SHA-1). A KAT performed on the DES or Triple-DES algorithms adequately verifies their associated hashing algorithm. This is not the case for the keyed hashing algorithm using a SHS algorithm which implements several other functions in addition to the underlying SHS algorithm.

Additional Comments

As discussed in FIPS 140-2 IG 9.3, if HMAC-SHA-1 is used as the Approved integrity technique to verify the software or firmware components as specified in AS.06.08, a KAT is not required for either the HMAC-SHA-1 or the underlying SHA-1 algorithm.

9.2 Known Answer Test for Embedded Cryptographic Algorithms

Applicable Levels:	*All*
Effective Dates:	*2/10/2004*
Last Modified:	*8/19/2004*
Relevant Assertions:	*AS.09.19*
Relevant Test Requirements:	*TE.09.19.01, 02 and 03*
Relevant Vendor Requirements:	*VE.09.19.01 and 02*

Background

Core cryptographic algorithms are often embedded into other higher cryptographic algorithms for their operation in FIPS mode (e.g. SHA-1 algorithm embedded into HMAC-SHA-1 and DSA, DES or Triple-DES into RNGs). FIPS 140-2 requires that cryptographic modules that implement FIPS-approved algorithms used in FIPS mode perform a Known-Answer-Test (KAT) as part of their power-up self-tests. This requirement is also valid for the core cryptographic algorithm implementation. However, when the cryptographic module performs the KAT on the higher cryptographic algorithm, the embedded core cryptographic algorithm may also be self-tested.

Question/Problem

If an embedded core cryptographic algorithm is self-tested during the higher cryptographic algorithm KAT, is it necessary for the cryptographic module to implement a KAT for the already self-tested core cryptographic algorithm implementation?

Resolution

It is acceptable for the cryptographic module not to perform a KAT on the embedded core cryptographic algorithm implementation if;

1. the higher cryptographic algorithm uses that implementation,
2. the higher cryptographic algorithm performs a KAT at power-up and,
3. all cryptographic functions within the core cryptographic algorithm are tested (e.g. encryption and decryption for DES and Triple-DES).

Additional Comments

If the cryptographic module contains several core cryptographic algorithm implementations (e.g., several different implementations of SHA-1 algorithm) and some are not used by other higher FIPS-approved cryptographic algorithms (and are therefore not self-tested), then the cryptographic module must perform a KAT at power-up for each of those implementations.

Implementation of DES or Triple-DES within an RNG such as ANSI X9.31 does not meet bullet #3 above since not all the DES or Triple-DES cryptographic functions are tested (e.g. encrypt is performed in the RNG generation, not decrypt)

Implementation of SHA-1 within the FIPS 186-2 random number generation algorithms does not meet bullet #3 above since the hashing function is not completely performed

9.3 KAT for Algorithms used in an Integrity Test Technique

Applicable Levels:	*ALL*
Effective Dates:	*2/10/2004*
Last Modified:	
Relevant Assertions:	*AS06.08 and AS09.16*
Relevant Test Requirements:	*TE06.08.01 - 02 and TE09.16.01 - 02*
Relevant Vendor Requirements:	*VE06.08.01 and VE09.16.01*

Background

AS06.08 requires that a cryptographic mechanism using an Approved integrity technique shall be applied to all cryptographic software and firmware components within the cryptographic module. AS09.16 requires that a cryptographic algorithm test using a Known-Answer-Test (KAT) shall be conducted for all cryptographic functions of each Approved cryptographic algorithm implemented by the cryptographic module and used in FIPS mode of operation.

Question/Problem

Must a cryptographic module implement a separate KAT for the underlying cryptographic algorithm used in the Approved integrity technique?

Resolution

A cryptographic module may not implement a separate KAT for the underlying cryptographic algorithm used for the Approved integrity technique if all the cryptographic functions of the underlying cryptographic algorithm are tested (e.g. encryption and decryption for Triple-DES).

Rationale

The software/firmware integrity check using an Approved integrity technique is considered a KAT since the cryptographic module uses itself as an input to the algorithm and a known answer as the expected output.

EX: If HMAC-SHA-1 is used as the Approved integrity technique to verify the software or firmware components, a KAT is not required for either the HMAC-SHA-1 or the underlying SHA-1 algorithm.

EX: If Triple-DES MAC is used as the Approved integrity technique to verify the software or firmware components, a KAT is still required for the underlying Triple-DES as the integrity checking may not use both the Triple-DES encrypt and decrypt functions.

EX: If RSA is used to verify the signature of the software or firmware components, a KAT is still required for the underlying RSA as the integrity checking would not use the RSA signature generation function. However, a KAT for the underlying SHA-1 hashing function is not required.

Additional Comments

9.4 Cryptographic Algorithm Tests for SHS Algorithms and Higher Cryptographic Algorithms Using SHS Algorithms

Applicable Levels:	*ALL*
Effective Dates:	*8/19/2004*
Last Modified:	
Relevant Assertions:	*AS09.16*
Relevant Test Requirements:	*TE09.16.01*
Relevant Vendor Requirements:	*VE09.16.01*

Background

Cryptographic algorithm test. A cryptographic algorithm test using a known answer shall be conducted for all cryptographic functions (e.g., encryption, decryption, authentication, and random number generation) of each Approved cryptographic algorithm implemented by a cryptographic module. A known-answer test involves operating the cryptographic algorithm on data for which the correct output is already known and comparing the calculated output with the previously generated output (the known answer). If the calculated output does not equal the known answer, the known-answer test shall fail.

Cryptographic algorithms whose outputs vary for a given set of inputs (e.g., the Digital Signature Algorithm) shall be tested using a known-answer test or shall be tested using a pair-wise consistency test (specified below).

Each algorithm implementation to be used in a FIPS Approved mode of operation must implement a cryptographic algorithm test. The cryptographic algorithm test is a *health check* of the algorithm implementation performed at power-up or on demand.

Question/Problem

What are the minimum requirements placed on Known Answer Tests (KATs) for SHS algorithms and higher cryptographic algorithms implementing SHS algorithms so that they can be used in FIPS Approved mode of operation? What are the minimum requirements placed on a pair-wise consistency test (for public and private keys) if performed at power-up or on demand?

Resolution

Following is a subset of algorithm KAT specific implementation guidance:

- the following are minimal requirements for SHS algorithms:
  - a KAT for SHA-1 (if applicable) is required;
  - a KAT for SHA-256 (if applicable) is required;
  - a KAT for SHA-224 (if applicable) is required if SHA-224 is implemented without SHA-256;
  - a KAT for SHA-512 (if applicable) is required; and,
  - a KAT for SHA-384 (if applicable) is required if SHA-384 is implemented without SHA-512.

- a KAT or pair-wise consistency for DSA and RSA (if applicable) is required and shall be performed on:
  - at minimum, the smallest NIST-Recommended modulus size that is supported by the module; and,
  - at minimum, any one of the implemented underlying SHS algorithms used by the higher cryptographic algorithm.

- a KAT or pair-wise consistency for ECDSA (if applicable) is required and shall be performed at a minimum, on:

  - any one of the implemented curves in each of the implemented two types of fields (i.e., prime field where *GF(p)*, and binary field where $GF(2^m)$); and
  - any one of the implemented underlying SHS algorithms used by the higher cryptographic algorithm.

- a KAT for HMAC (if applicable) is required and shall be performed at minimum, on any one of the implemented underlying SHS algorithms.

Additional Comments

FIPS 140-2 IG 9.2 *Known Answer Test for Embedded Crypto Algorithms* applies.

This IG is consistent with FIPS 140-2 IG 9.1 *Known Answer Test For Keyed Hashing Algorithm.*

Rationale: The purpose of a KAT is to perform a health-check of the cryptographic module to identify catastrophic failures or alterations of the module between power cycles and not that the implementation is correct. The implementation verification is performed during the cryptographic algorithmic testing and validation.

Section 10 – Design Assurance

Section 11 – Mitigation of Other Attacks

Section 12 – Appendix A: Summary of Documentation Requirements

Section 13 – Appendix B: Recommended Software Development Practices

Section 14 – Appendix C: Cryptographic Module Security Policy

14.1 Level Of Detail When Reporting Cryptographic Services

Applicable Levels:	*ALL*
Effective Dates:	*11/15/2001*
Last Modified:	
Relevant Assertions:	*AS01.02, AS01.03, AS01.12, AS01.16, AS03.14, AS10.06, AS14.02, AS14.03, AS14.04, AS14.06, AS14.07*
Relevant Test Requirements:	*TE01.03.01, TE01.03.02, TE01.16.01, TE03.14.01, TE10.06.01, TE14.07.01, TE14.07.02*
Relevant Vendor Requirements:	*VE01.03.01, VE01.03.02, VE01.16.01, VE03.14.01, VE03.14.02, VE10.06.01, VE14.07.01, VE14.07.02, VE14.07.03*

Question/Problem

What is the level of detail that the non-proprietary security policy must contain in order to describe the cryptographic service(s) implemented by a cryptographic module?

Resolution

When presenting information in the non-proprietary security policy regarding the cryptographic services that are included in the module validation, the security policy shall include, at a minimum, the following information **for each service:**

- The service name
- A concise description of the service purpose and/or use (the service name alone may, in some instances, provide this information)
- A list of Approved security functions (algorithm(s), key management technique(s) or authentication technique) used by, or implemented through, the invocation of the service.
- A list of the cryptographic keys and/or CSPs associated with the service or with the Approved security function(s) it uses.
- For each operator role authorized to use the service:
    - Information describing the individual access rights to all keys and/or CSPs
    - Information describing the method used to authenticate each role.

The presentation style of the documentation is left to the vendor. FIPS 140-2, Appendix C, contains tabular templates that provide non-exhaustive samples and illustrations as to the kind of information to be included in meeting the documentation requirements of the Standard.

Additional Comments

FIPS 140-2 requires information to be included in the module security policy which:

- Allows a user (operator) to determine when an approved mode of operation is selected (**AS01.06, AS01.16**).

- Lists all security services, operations or functions, both Approved and non-Approved, that are provided by the cryptographic module and available to operators (**AS01.12, AS03.07, AS03.14, AS14.03**).

- Provides a correspondence between the module hardware, software, and firmware components (**AS10.06**)

- Provides a specification of the security rules under which the module shall operate, including the security rules derived from the requirements of FIPS 140-2. (**AS14.02**)

- For each service, specifies a detailed specification of the service inputs, corresponding service outputs, and the authorized roles in which the service can be performed. **(AS03.14, AS14.03)**

See also the definitions of ***Approved mode of operation*** and ***Approved security function*** in FIPS 140-2.

14.2 Level Of Detail When Reporting Mitigation Of Attacks

Applicable Levels:	*ALL*
Effective Dates:	*11/15/2001*
Last Modified:	
Relevant Assertions:	*AS 14.09*
Relevant Test Requirements:	*TE14.09.01*
Relevant Vendor Requirements:	*VE14.09.01*

Question/Problem

What is the level of detail that the non-proprietary security policy must contain that describes the security mechanism(s) implemented by the cryptographic module to mitigate other attacks?

Resolution

The level of detail describing the security mechanism(s) implemented by the cryptographic module to mitigate other attacks required to be contained in the security policy must be similar to what is found on advertisement documentation (product glossies).

Additional Comments

Expired Implementation Guidance

End of Document